An effective bound of p for algebraic points on Shimura curves of $\Gamma_0(p)$-type

Keisuke Arai

Abstract

In previous articles, we classified the characters associated to algebraic points on Shimura curves of $\Gamma_0(p)$-type, and over number fields in a certain large class we showed that there are at most elliptic points on such a Shimura curve for every sufficiently large prime number p. In this article, we obtain an effective bound of p concerning algebraic points on Shimura curves of $\Gamma_0(p)$-type.

Notation

For an integer $n \geq 1$ and a commutative group (or a commutative group scheme) G, let $G[n]$ denote the kernel of multiplication by n in G. For a field F, let $\mathrm{char}\, F$ denote the characteristic of F, let $\overline{F}$ denote an algebraic closure of F, let F^{sep} (resp. F^{ab}) denote the separable closure (resp. the maximal abelian extension) of F inside $\overline{F}$, and let $\mathrm{G}_F = \mathrm{Gal}(F^{\mathrm{sep}}/F)$, $\mathrm{G}_F^{\mathrm{ab}} = \mathrm{Gal}(F^{\mathrm{ab}}/F)$. For a prime number p and a field F of characteristic 0, let $\theta_p : \mathrm{G}_F \longrightarrow \mathbb{F}_p^\times$ denote the mod p cyclotomic character. Let $|\cdot|$ denote the usual complex absolute value on $\mathbb{C}$. For a number field or a local field k, let $\mathcal{O}_k$ denote the ring of integers of k. For a number field k, put $n_k := [k : \mathbb{Q}]$; let d_k denote the discriminant of k; let h_k denote the class number of k; let r_k denote the rank of the unit group $\mathcal{O}_k^\times$; let R_k denote the regulator of k; fix an inclusion $k \hookrightarrow \mathbb{C}$ and take the algebraic closure $\overline{k}$ inside $\mathbb{C}$; let k_v denote the completion of k at v where v is a place (or a prime) of k; let $k_{\mathbb{A}}$ denote the adèle ring of k; and let $\mathbf{Ram}(k)$ denote the set of prime numbers which are ramified in k. For a scheme S and an abelian scheme A over S, let $\mathrm{End}_S(A)$ denote the ring of endomorphisms of A defined over S. If $S = \mathrm{Spec}(F)$ for a field F and if F'/F is a field extension, simply put $\mathrm{End}_{F'}(A) := \mathrm{End}_{\mathrm{Spec}(F')}(A \times_{\mathrm{Spec}(F)} \mathrm{Spec}(F'))$ and $\mathrm{End}(A) := \mathrm{End}_{\overline{F}}(A)$. Let $\mathrm{Aut}(A) := \mathrm{Aut}_{\overline{F}}(A)$ be the group of automorphisms of A defined over $\overline{F}$. For a prime number p and an abelian variety A over a field F, let $T_pA := \varprojlim A[p^n](\overline{F})$ be the p-adic Tate module of A, where the inverse limit is taken with respect to multiplication by $p : A[p^{n+1}](\overline{F}) \longrightarrow A[p^n](\overline{F})$.

1 Introduction

Let B be an indefinite quaternion division algebra over $\mathbb{Q}$. Let

$$d := \mathrm{disc}\, B$$

be the discriminant of B. Then d is the product of an even number of distinct prime numbers, and $d > 1$. Fix a maximal order $\mathcal{O}$ of B. For each prime number p not dividing d, fix an isomorphism

$$\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathrm{M}_2(\mathbb{Z}_p) \tag{1.1}$$

of $\mathbb{Z}_p$-algebras.

Definition 1.1. (cf. [7, p.591]) Let S be a scheme. A QM-abelian surface by $\mathcal{O}$ over S is a pair (A, i) where A is an abelian surface over S (i.e. A is an abelian scheme over S of relative dimension 2), and $i : \mathcal{O} \hookrightarrow \mathrm{End}_S(A)$ is an injective ring homomorphism (sending 1 to id). We assume that A has a left $\mathcal{O}$-action. We will sometimes omit "by $\mathcal{O}$" and simply write "a QM-abelian surface" if there is no fear of confusion.

Let M^B be the coarse moduli scheme over $\mathbb{Q}$ parameterizing isomorphism classes of QM-abelian surfaces by $\mathcal{O}$. The notation M^B is permissible although we should write $M^{\mathcal{O}}$ instead of M^B; for even if we replace $\mathcal{O}$ by another maximal order $\mathcal{O}'$, we have a natural isomorphism $M^{\mathcal{O}} \cong M^{\mathcal{O}'}$ since $\mathcal{O}$ and $\mathcal{O}'$ are conjugate in B. Then M^B is a proper smooth curve over $\mathbb{Q}$, called a Shimura curve. For a prime number p not dividing d, let $M_0^B(p)$ be the coarse moduli scheme over $\mathbb{Q}$ parameterizing isomorphism classes of triples (A, i, V) where (A, i) is a QM-abelian surface by $\mathcal{O}$ and V is a left $\mathcal{O}$-submodule of $A[p]$ with $\mathbb{F}_p$-dimension 2. Then $M_0^B(p)$ is a proper smooth curve over $\mathbb{Q}$, which we call a Shimura curve of $\Gamma_0(p)$-type. We have a natural map

$$\pi^B(p) : M_0^B(p) \longrightarrow M^B$$

over $\mathbb{Q}$ defined by $(A, i, V) \longmapsto (A, i)$.

For real points on M^B, we know the following.

Theorem 1.2 ([14, Theorem 0, p.136])**.** *We have $M^B(\mathbb{R}) = \emptyset$.*

In the previous article, we showed that there are few points on $M_0^B(p)$ for every sufficiently large prime number p, which is an analogue of the study of points on the modular curve $X_0(p)$ ([12], [13]; for related topics, see [2]).

Theorem 1.3 ([3, Theorem 1.4])**.** *Let k be a finite Galois extension of $\mathbb{Q}$ which does not contain the Hilbert class field of any imaginary quadratic field. Then there is a finite set $\mathcal{L}(k)$ of prime numbers depending on k which satisfies the following. Assume that there is a prime number q which splits completely in k and satisfies $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \not\cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-q}))$, and let $p > 4q$ be a prime number which also satisfies $p \geq 11$, $p \neq 13$, $p \nmid d$ and $p \notin \mathcal{L}(k)$.*

(1) If $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$, then $M_0^B(p)(k) = \emptyset$.

(2) If $B \otimes_{\mathbb{Q}} k \not\cong \mathrm{M}_2(k)$, then $M_0^B(p)(k) \subseteq \{$elliptic points of order 2 or $3\}$.

We can identify $M_0^B(p)(\mathbb{C})$ with a quotient of the upper half-plane, and we use the notion of "elliptic points" in this context. In Theorem 1.3, the set $\mathcal{L}(k)$ can be described explicitly. In this article, we modify the set $\mathcal{L}(k)$ slightly, and obtain its effective bound in Section 7.

2 Galois representations associated to QM-abelian surfaces (generalities)

We consider the Galois representation associated to a QM-abelian surface. Take a prime number p not dividing d. Let F be a field with $\operatorname{char} F \neq p$. Let (A, i) be a QM-abelian surface by $\mathcal{O}$ over F. We have isomorphisms of $\mathbb{Z}_p$-modules:

$$\mathbb{Z}_p^4 \cong T_pA \cong \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathrm{M}_2(\mathbb{Z}_p).$$

The middle is also an isomorphism of left $\mathcal{O}$-modules; the last is also an isomorphism of $\mathbb{Z}_p$-algebras (which is fixed in (1.1)). We sometimes identify these $\mathbb{Z}_p$-modules. Take a $\mathbb{Z}_p$-basis

$$e_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},\ e_2 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},\ e_3 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\ e_4 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

of $\mathrm{M}_2(\mathbb{Z}_p)$. Then the image of the natural map

$$\mathrm{M}_2(\mathbb{Z}_p) \cong \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p \hookrightarrow \mathrm{End}(T_pA) \cong \mathrm{M}_4(\mathbb{Z}_p)$$

lies in $\left\{ \begin{pmatrix} X & 0 \\ 0 & X \end{pmatrix} \middle| X \in \mathrm{M}_2(\mathbb{Z}_p) \right\}$. The action of the Galois group G_F on T_pA induces a representation

$$\rho : \mathrm{G}_F \longrightarrow \mathrm{Aut}_{\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{Z}_p}(T_pA) \subseteq \mathrm{Aut}(T_pA) \cong \mathrm{GL}_4(\mathbb{Z}_p),$$

where $\mathrm{Aut}_{\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{Z}_p}(T_pA)$ is the group of automorphisms of T_pA commuting with the action of $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$. We often identify $\mathrm{Aut}(T_pA) = \mathrm{GL}_4(\mathbb{Z}_p)$. The above observation implies

$$\mathrm{Aut}_{\mathcal{O}\otimes_{\mathbb{Z}}\mathbb{Z}_p}(T_pA) = \left\{ \begin{pmatrix} sI_2 & tI_2 \\ uI_2 & vI_2 \end{pmatrix} \middle| \begin{pmatrix} s & t \\ u & v \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_p) \right\},$$

where $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Then the Galois representation ρ factors as

$$\rho : \mathrm{G}_F \longrightarrow \left\{ \begin{pmatrix} sI_2 & tI_2 \\ uI_2 & vI_2 \end{pmatrix} \middle| \begin{pmatrix} s & t \\ u & v \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_p) \right\} \subseteq \mathrm{GL}_4(\mathbb{Z}_p).$$

Let

$$\overline{\rho} : \mathrm{G}_F \longrightarrow \left\{ \begin{pmatrix} sI_2 & tI_2 \\ uI_2 & vI_2 \end{pmatrix} \middle| \begin{pmatrix} s & t \\ u & v \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p) \right\} \subseteq \mathrm{GL}_4(\mathbb{F}_p)$$

be the reduction of ρ modulo p. Let

$$\overline{\rho}_{A,p} : \mathrm{G}_F \longrightarrow \mathrm{GL}_2(\mathbb{F}_p) \tag{2.1}$$

denote the Galois representation induced from $\overline{\rho}$ by "$\begin{pmatrix} s & t \\ u & v \end{pmatrix}$", so that we have $\overline{\rho}_{A,p}(\sigma) = \begin{pmatrix} s & t \\ u & v \end{pmatrix}$ if $\overline{\rho}(\sigma) = \begin{pmatrix} sI_2 & tI_2 \\ uI_2 & vI_2 \end{pmatrix}$ for $\sigma \in \mathrm{G}_F$.

Suppose that $A[p](F^{\mathrm{sep}})$ has a left $\mathcal{O}$-submodule V with $\mathbb{F}_p$-dimension 2 which is stable under the action of G_F. We may assume $V = \mathbb{F}_p e_1 \oplus \mathbb{F}_p e_2 = \left\{ \begin{pmatrix} * & 0 \\ * & 0 \end{pmatrix} \right\}$. Since V is stable under the action of G_F, we find $\overline{\rho}_{A,p}(\mathrm{G}_F) \subseteq \left\{ \begin{pmatrix} s & t \\ 0 & v \end{pmatrix} \right\} \subseteq \mathrm{GL}_2(\mathbb{F}_p)$. Let

$$\lambda : \mathrm{G}_F \longrightarrow \mathbb{F}_p^\times \tag{2.2}$$

denote the character induced from $\overline{\rho}_{A,p}$ by "s", so that $\overline{\rho}_{A,p}(\sigma) = \begin{pmatrix} \lambda(\sigma) & * \\ 0 & * \end{pmatrix}$ for $\sigma \in \mathrm{G}_F$. Note that G_F acts on V by λ (i.e. $\overline{\rho}(\sigma)(v) = \lambda(\sigma)v$ for $\sigma \in \mathrm{G}_F$, $v \in V$).

3 Automorphism groups

We consider the automorphism group of a QM-abelian surface. Let (A, i) be a QM-abelian surface by $\mathcal{O}$ over a field F. Put

$$\mathrm{End}_{\mathcal{O}}(A) := \{ f \in \mathrm{End}(A) \mid f i(g) = i(g) f \ \text{ for any } g \in \mathcal{O} \}$$

and

$$\mathrm{Aut}_{\mathcal{O}}(A) := \mathrm{Aut}(A) \cap \mathrm{End}_{\mathcal{O}}(A).$$

If $\mathrm{char}\, F = 0$, then $\mathrm{Aut}_{\mathcal{O}}(A) \cong \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/6\mathbb{Z}$.

Let p be a prime number not dividing d. Let (A, i, V) be a triple where (A, i) is a QM-abelian surface by $\mathcal{O}$ over a field F and V is a left $\mathcal{O}$-submodule of $A[p](\overline{F})$ with $\mathbb{F}_p$-dimension 2. Define a subgroup $\mathrm{Aut}_{\mathcal{O}}(A, V)$ of $\mathrm{Aut}_{\mathcal{O}}(A)$ by

$$\mathrm{Aut}_{\mathcal{O}}(A, V) := \{ f \in \mathrm{Aut}_{\mathcal{O}}(A) \mid f(V) = V \}.$$

Assume $\mathrm{char}\, F = 0$. Then $\mathrm{Aut}_{\mathcal{O}}(A, V) \cong \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/6\mathbb{Z}$. Notice that we have $\mathrm{Aut}_{\mathcal{O}}(A) \cong \mathbb{Z}/2\mathbb{Z}$ (resp. $\mathrm{Aut}_{\mathcal{O}}(A, V) \cong \mathbb{Z}/2\mathbb{Z}$) if and only if $\mathrm{Aut}_{\mathcal{O}}(A) = \{\pm 1\}$ (resp. $\mathrm{Aut}_{\mathcal{O}}(A, V) = \{\pm 1\}$).

4 Fields of definition

Let k be a number field. Let p be a prime number not dividing d. Take a point

$$x \in M_0^B(p)(k).$$

Let $x' \in M^B(k)$ be the image of x by the map $\pi^B(p) : M_0^B(p) \longrightarrow M^B$. Then x' is represented by a QM-abelian surface (say (A_x, i_x)) over $\overline{k}$, and x is represented by a triple (A_x, i_x, V_x) where V_x is a left $\mathcal{O}$-submodule of $A[p](\overline{k})$ with $\mathbb{F}_p$-dimension 2. For a finite extension M of k (in $\overline{k}$), we say that we can take (A_x, i_x) (resp. (A_x, i_x, V_x)) to be defined over M if there is a QM-abelian surface (A, i) over M such that $(A, i) \otimes_M \overline{k}$ is isomorphic to (A_x, i_x) (resp. if there is a QM-abelian surface (A, i) over M and a left $\mathcal{O}$-submodule V of $A[p](\overline{k})$ with $\mathbb{F}_p$-dimension 2 stable under

the action of G_M such that there is an isomorphism between $(A, i) \otimes_M \overline{k}$ and (A_x, i_x) under which V corresponds to V_x). Put

$$\mathrm{Aut}(x) := \mathrm{Aut}_{\mathcal{O}}(A_x, V_x), \quad \mathrm{Aut}(x') := \mathrm{Aut}_{\mathcal{O}}(A_x).$$

Then $\mathrm{Aut}(x)$ is a subgroup of $\mathrm{Aut}(x')$. Note that x is an elliptic point of order 2 (resp. 3) if and only if $\mathrm{Aut}(x) \cong \mathbb{Z}/4\mathbb{Z}$ (resp. $\mathrm{Aut}(x) \cong \mathbb{Z}/6\mathbb{Z}$).

Since x is a k-rational point, we have ${}^{\sigma}x = x$ for any $\sigma \in \mathrm{G}_k$. Then, for any $\sigma \in \mathrm{G}_k$, there is an isomorphism

$$\phi_\sigma : {}^{\sigma}(A_x, i_x, V_x) \longrightarrow (A_x, i_x, V_x),$$

which we fix once for all. Let

$$\phi'_\sigma : {}^{\sigma}(A_x, i_x) \longrightarrow (A_x, i_x)$$

be the isomorphism induced from ϕ_σ by forgetting V_x. For $\sigma, \tau \in \mathrm{G}_k$, put

$$c_x(\sigma, \tau) := \phi_\sigma \circ {}^{\sigma}\phi_\tau \circ \phi_{\sigma\tau}^{-1} \in \mathrm{Aut}(x)$$

and

$$c'_x(\sigma, \tau) := \phi'_\sigma \circ {}^{\sigma}\phi'_\tau \circ (\phi'_{\sigma\tau})^{-1} \in \mathrm{Aut}(x').$$

Then c_x (resp. c'_x) is a 2-cocycle and defines a cohomology class $[c_x] \in H^2(\mathrm{G}_k, \mathrm{Aut}(x))$ (resp. $[c'_x] \in H^2(\mathrm{G}_k, \mathrm{Aut}(x'))$). Here the action of G_k on $\mathrm{Aut}(x)$ (resp. $\mathrm{Aut}(x')$) is defined in a natural manner (cf. [4, Section 4]).

Proposition 4.1 ([9, Theorem (1.1), p.93])**.** *We can take (A_x, i_x) to be defined over k if and only if $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$.*

Proposition 4.2 ([4, Proposition 4.2])**.** *(1) Suppose $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$. Further assume $\mathrm{Aut}(x) \neq \{\pm 1\}$ or $\mathrm{Aut}(x') \not\cong \mathbb{Z}/4\mathbb{Z}$. Then we can take (A_x, i_x, V_x) to be defined over k.*

(2) Assume $\mathrm{Aut}(x) = \{\pm 1\}$. Then there is a quadratic extension K of k such that we can take (A_x, i_x, V_x) to be defined over K.

Lemma 4.3 ([4, Lemma 4.3])**.** *Let K be a quadratic extension of k. Assume $\mathrm{Aut}(x) = \{\pm 1\}$. Then the following two conditions are equivalent.*

(1) We can take (A_x, i_x, V_x) to be defined over K.

(2) For any place v of k satisfying $[c_x]_v \neq 0$, the tensor product $K \otimes_k k_v$ is a field.

5 Classification of characters

We keep the notation in Section 4. Throughout this section, assume $\mathrm{Aut}(x) = \{\pm 1\}$. Let K be a quadratic extension of k which satisfies the equivalent conditions in Lemma 4.3. Then x is represented by a triple (A, i, V), where (A, i) is a QM-abelian

surface over K and V is a left $\mathcal{O}$-submodule of $A[p](\overline{K})$ with $\mathbb{F}_p$-dimension 2 stable under the action of G_K. Let

$$\lambda : \mathrm{G}_K \longrightarrow \mathbb{F}_p^{\times}$$

be the character associated to V in (2.2). For a prime $\mathfrak{l}$ of k (resp. K), let $I_{\mathfrak{l}}$ denote the inertia subgroup of G_k (resp. G_K) at $\mathfrak{l}$.

Let $\lambda^{\mathrm{ab}} : \mathrm{G}_K^{\mathrm{ab}} \longrightarrow \mathbb{F}_p^{\times}$ be the natural map induced from λ. Put

$$\varphi := \lambda^{\mathrm{ab}} \circ \mathrm{tr}_{K/k} : \mathrm{G}_k \longrightarrow \mathrm{G}_K^{\mathrm{ab}} \longrightarrow \mathbb{F}_p^{\times} \tag{5.1}$$

where $\mathrm{tr}_{K/k} : \mathrm{G}_k \longrightarrow \mathrm{G}_K^{\mathrm{ab}}$ is the transfer map. Notice that the induced map $\mathrm{tr}_{K/k}^{\mathrm{ab}} : \mathrm{G}_k^{\mathrm{ab}} \longrightarrow \mathrm{G}_K^{\mathrm{ab}}$ from $\mathrm{tr}_{K/k}$ corresponds to the natural inclusion $k_{\mathbb{A}}^{\times} \hookrightarrow K_{\mathbb{A}}^{\times}$ via class field theory ([15, Theorem 8 in §9 of Chapter XIII, p.276]). We know that φ^{12} is unramified at every prime of k not dividing p ([4, Corollary 5.2]), and so φ^{12} corresponds to a character of the ideal group $\mathfrak{I}_k(p)$ consisting of fractional ideals of k prime to p. By abuse of notation, let φ^{12} also denote the corresponding character of $\mathfrak{I}_k(p)$.

Let $\mathcal{M}^{new}$ be the set of prime numbers q such that q splits completely in k. Let $\mathcal{N}^{new}$ be the set of primes $\mathfrak{q}$ of k such that $\mathfrak{q}$ divides some prime number $q \in \mathcal{M}^{new}$. Take a finite subset $\emptyset \neq \mathcal{S}^{new} \subseteq \mathcal{N}^{new}$ which generates the ideal class group of k. For each prime $\mathfrak{q} \in \mathcal{S}^{new}$, fix an element $\alpha_{\mathfrak{q}} \in \mathcal{O}_k \setminus \{0\}$ satisfying $\mathfrak{q}^{h_k} = \alpha_{\mathfrak{q}}\mathcal{O}_k$.

For an integer $n \geq 1$, put

$$\mathcal{FR}(n) := \left\{ \beta \in \mathbb{C} \;\middle|\; \beta^2 + a\beta + n = 0 \text{ for some integer } a \in \mathbb{Z} \text{ with } |a| \leq 2\sqrt{n} \right\}.$$

For any element $\beta \in \mathcal{FR}(n)$, we have $|\beta| = \sqrt{n}$. For a prime $\mathfrak{q}$ of k, put $\mathrm{N}(\mathfrak{q}) = \sharp(\mathcal{O}_k/\mathfrak{q})$. If $\mathfrak{q} \in \mathcal{S}^{new}$, then $\mathrm{N}(\mathfrak{q})$ is a prime number. Define the sets

$$\mathcal{E}(k) := \left\{ \varepsilon_0 = \sum_{\sigma \in \mathrm{Gal}(k/\mathbb{Q})} a_\sigma \sigma \in \mathbb{Z}[\mathrm{Gal}(k/\mathbb{Q})] \;\middle|\; a_\sigma \in \{0, 8, 12, 16, 24\} \right\},$$
$$\mathcal{M}_1^{new}(k) := \{ (\mathfrak{q}, \varepsilon_0, \beta_{\mathfrak{q}}) \mid \mathfrak{q} \in \mathcal{S}^{new},\ \varepsilon_0 \in \mathcal{E}(k),\ \beta_{\mathfrak{q}} \in \mathcal{FR}(\mathrm{N}(\mathfrak{q})) \},$$
$$\mathcal{M}_2^{new}(k) := \left\{ \mathrm{Norm}_{k(\beta_{\mathfrak{q}})/\mathbb{Q}}(\alpha_{\mathfrak{q}}^{\varepsilon_0} - \beta_{\mathfrak{q}}^{24h_k}) \in \mathbb{Z} \;\middle|\; (\mathfrak{q}, \varepsilon_0, \beta_{\mathfrak{q}}) \in \mathcal{M}_1^{new}(k) \right\} \setminus \{0\},$$
$$\mathcal{N}_0^{new}(k) := \{ l : \text{prime number} \mid l \text{ divides some integer } m \in \mathcal{M}_2^{new}(k) \},$$
$$\mathcal{T}^{new}(k) := \{ l' : \text{prime number} \mid l' \text{ is divisible by some prime } \mathfrak{q}' \in \mathcal{S}^{new} \} \cup \{2, 3\},$$
$$\mathcal{N}_1^{new}(k) := \mathcal{N}_0^{new}(k) \cup \mathcal{T}^{new}(k) \cup \mathbf{Ram}(k).$$

Note that all the sets, $\mathcal{FR}(n)$, $\mathcal{M}_1^{new}(k)$, $\mathcal{M}_2^{new}(k)$, $\mathcal{N}_0^{new}(k)$, $\mathcal{T}^{new}(k)$, and $\mathcal{N}_1^{new}(k)$, are finite.

Theorem 5.1 (cf. [4, Theorem 5.6]). *Assume that k is Galois over $\mathbb{Q}$. If $p \notin \mathcal{N}_1^{new}(k)$ (and if p does not divide d), then the character $\varphi : \mathrm{G}_k \longrightarrow \mathbb{F}_p^{\times}$ is of one of the following types.*

Type 2: $\varphi^{12} = \theta_p^{12}$ and $p \equiv 3 \bmod 4$.

Type 3: There is an imaginary quadratic field L satisfying the following two conditions.
(a) The Hilbert class field H_L of L is contained in k.
(b) There is a prime $\mathfrak{p}_L$ of L lying over p such that $\varphi^{12}(\mathfrak{a}) \equiv \delta^{24} \bmod \mathfrak{p}_L$ holds for any fractional ideal $\mathfrak{a}$ of k prime to p. Here δ is any element of L such that $\mathrm{Norm}_{k/L}(\mathfrak{a}) = \delta\mathcal{O}_L$.

Proof. It suffices to modify the proof of Theorem 5.6 in [4] slightly. First, notice that the abelian surface $A \otimes_K K_{\mathfrak{q}_K}$ over $K_{\mathfrak{q}_K}$ (which corresponds to $x \otimes K_{\mathfrak{q}_K}$) has good reduction after a totally ramified finite extension $M(\mathfrak{q})/K_{\mathfrak{q}_K}$ without assuming $q \geq 5$ ([9, Proposition 3.2, p.101]). Second, in the case where ε is of type 2, notice that $\beta_{\mathfrak{q}}^{24h_k} = q^{12h_k}$ implies $\beta_{\mathfrak{q}}^{24} = q^{12}$ without assuming $q \nmid 6h_k$. Now we show this. Write $\beta = \beta_{\mathfrak{q}}$ for simplicity. Let $\overline{\beta}$ be the complex conjugate of β. Since $\beta^{24h_k} = \overline{\beta}^{24h_k}$, we have $\overline{\beta} = \zeta\beta$ for some $\zeta \in \mathbb{C}$ with $\zeta^{24h_k} = 1$. Since $\mathbb{Q}(\beta) = \mathbb{Q}(\overline{\beta}) = \mathbb{Q}(\zeta\beta) = \mathbb{Q}(\beta, \zeta) \supseteq \mathbb{Q}(\zeta)$ and $[\mathbb{Q}(\beta) : \mathbb{Q}] = 2$, we have $\zeta^4 = 1$ or $\zeta^6 = 1$. Then $\zeta^{12} = 1$. This implies $\overline{\beta}^{12} = \zeta^{12}\beta^{12} = \beta^{12}$, and so $\beta^{12} \in \mathbb{Q}$. Since $|\beta| = \sqrt{q}$, we have $\beta^{12} = \pm q^6$, and hence $\beta^{24} = q^{12}$. Notice that the case $\beta^{12} = -q^6$ really occurs (e.g. $q = 2$ and $\beta = 1 + \sqrt{-1}$).

□

From now to the end of this section, assume that k is Galois over $\mathbb{Q}$. The set $\mathcal{N}_1^{new}(k)$ may differ from $\mathcal{N}_1(k)$ in [4], nevertheless we have the following.

Lemma 5.2 (cf. [5, Lemma 5.11])**.** *Suppose $p \geq 11$, $p \neq 13$ and $p \notin \mathcal{N}_1^{new}(k)$. Further assume the following two conditions.*

(a) Every prime $\mathfrak{p}$ of k above p is inert in K/k.

(b) Every prime $\mathfrak{q} \in \mathcal{S}^{new}$ is ramified in K/k.

If φ is of type 2, then we have the following.

(i) The character $\lambda^{12}\theta_p^{-6} : \mathrm{G}_K \longrightarrow \mathbb{F}_p^\times$ is unramified everywhere.

(ii) The map $Cl_K \longrightarrow \mathbb{F}_p^\times$ induced from $\lambda^{12}\theta_p^{-6}$ is trivial on $C_{K/k} := \mathrm{Im}\,(Cl_k \longrightarrow Cl_K)$, where Cl_K is the ideal class group of K and $Cl_k \longrightarrow Cl_K$ is the map defined by $[\mathfrak{a}] \longmapsto [\mathfrak{a}\mathcal{O}_K]$.

Proof. (ii) The argument in the proof of Lemma 5.11 (ii) in [5] works here, but we may not have $\beta = \pm\sqrt{-q}$. Nevertheless we have $\beta^{24} = q^{12}$ as seen in the proof of Theorem 5.1, and so we are done.

□

We also have the following with the same proof as before.

Lemma 5.3 (cf. [3, Lemma 5.6], [4, Lemma 5.12], [5, 3])**.** *Suppose $p \geq 11$, $p \neq 13$ and $p \notin \mathcal{N}_1^{new}(k)$. Assume that φ is of type 2. Let $q < \frac{p}{4}$ be a prime number which splits completely in k. Then we have $\left(\frac{q}{p}\right) = -1$ and $q^{\frac{p-1}{2}} \equiv -1 \bmod p$. Furthermore, we have $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-q}))$.*

6 Irreducibility result

Let k be a number field, and let (A, i) be a QM-abelian surface by $\mathcal{O}$ over k. For a prime number p not dividing d, assume that the representation $\overline{\rho}_{A,p}$ in (2.1) is reducible. Then there is a 1-dimensional sub-representation of $\overline{\rho}_{A,p}$; let ν be its associated character. In this case notice that there is a left $\mathcal{O}$-submodule V of $A[p](\overline{k})$ with $\mathbb{F}_p$-dimension 2 on which G_k acts by ν, and so the triple (A, i, V) determines a point $x \in M_0^B(p)(k)$. Take any quadratic extension K of k. Then we have the

characters $\lambda : \mathrm{G}_K \longrightarrow \mathbb{F}_p^\times$ and $\varphi : \mathrm{G}_k \longrightarrow \mathbb{F}_p^\times$ associated to the triple $(A \otimes_k K, i, V)$. We know $\varphi = \nu^2$ by construction of φ.

Theorem 6.1. *Let k be a finite Galois extension of $\mathbb{Q}$ which does not contain the Hilbert class field of any imaginary quadratic field. Assume that there is a prime number q which splits completely in k and satisfies $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \not\cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-q}))$. Let $p > 4q$ be a prime number which also satisfies $p \geq 11$, $p \neq 13$, $p \nmid d$ and $p \notin \mathcal{N}_1^{new}(k)$. Then the representation*

$$\overline{\rho}_{A,p} : \mathrm{G}_k \longrightarrow \mathrm{GL}_2(\mathbb{F}_p)$$

is irreducible.

Proof. Assume that $\overline{\rho}_{A,p}$ is reducible. Then the associated character φ is of type 2 in Theorem 5.1, because k does not contain the Hilbert class field of any imaginary quadratic field. By Lemma 5.3, we have $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-q}))$, which is a contradiction.

□

Theorem 6.2. *Let k be a finite Galois extension of $\mathbb{Q}$ which does not contain the Hilbert class field of any imaginary quadratic field. Assume that there is a prime number q which splits completely in k and satisfies $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \not\cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-q}))$, and let $p > 4q$ be a prime number which also satisfies $p \geq 11$, $p \neq 13$, $p \nmid d$ and $p \notin \mathcal{N}_1^{new}(k)$.*

(1) If $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$, then $M_0^B(p)(k) = \emptyset$.

(2) If $B \otimes_{\mathbb{Q}} k \not\cong \mathrm{M}_2(k)$, then $M_0^B(p)(k) \subseteq \{$elliptic points of order 2 or 3$\}$.

(Proof of Theorem 6.2)

Let k be a finite Galois extension of $\mathbb{Q}$ which does not contain the Hilbert class field of any imaginary quadratic field, and let q be a prime number which splits completely in k and satisfies $B \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-q}) \not\cong \mathrm{M}_2(\mathbb{Q}(\sqrt{-q}))$. Let $p > 4q$ be a prime number which also satisfies $p \geq 11$, $p \neq 13$ and $p \nmid d$. Take a point $x \in M_0^B(p)(k)$.

(1) Suppose $B \otimes_{\mathbb{Q}} k \cong \mathrm{M}_2(k)$.

(1-i) Assume $\mathrm{Aut}(x) \neq \{\pm 1\}$ or $\mathrm{Aut}(x') \not\cong \mathbb{Z}/4\mathbb{Z}$. Then x is represented by a triple (A, i, V) defined over k by Proposition 4.2 (1), and the representation $\overline{\rho}_{A,p}$ is reducible. By Theorem 6.1, we have $p \in \mathcal{N}_1^{new}(k)$.

(1-ii) Assume otherwise (i.e. $\mathrm{Aut}(x) = \{\pm 1\}$ and $\mathrm{Aut}(x') \cong \mathbb{Z}/4\mathbb{Z}$). Then x is represented by a triple (A, i, V) defined over a quadratic extension of k by Proposition 4.2 (2), and we have a character $\varphi : \mathrm{G}_k \longrightarrow \mathbb{F}_p^\times$ as in (5.1). By Theorem 5.1 and Lemma 5.3, we have $p \in \mathcal{N}_1^{new}(k)$.

(2) Suppose $B \otimes_{\mathbb{Q}} k \not\cong \mathrm{M}_2(k)$. Further assume that x is not an elliptic point of order 2 or 3; this implies $\mathrm{Aut}(x) = \{\pm 1\}$. By the same argument as in (1-ii), we conclude $p \in \mathcal{N}_1^{new}(k)$.

□

7 Estimate of $\mathcal{N}_1^{new}(k)$

We estimate the set $\mathcal{N}_1^{new}(k)$ in the method of [8].

Theorem 7.1 ([11, Theorem 1.1, p.272]). *There is an absolute, effectively computable constant $A_1 > 1$ such that for every finite extension k_1 of $\mathbb{Q}$, every finite Galois extension k_2 of k_1 and every conjugacy class C of $\mathrm{Gal}(k_2/k_1)$, there is a prime $\mathfrak{q}$ of k_1 which is unramified in k_2, for which $\mathrm{Frob}_{\mathfrak{q}} = C$, for which $\mathrm{N}(\mathfrak{q})$ is a prime number, and which satisfies the bound $\mathrm{N}(\mathfrak{q}) \leq 2d_{k_2}^{A_1}$. Here $\mathrm{Frob}_{\mathfrak{q}}$ is the (arithmetic) Frobenius conjugacy class at $\mathfrak{q}$ in $\mathrm{Gal}(k_2/k_1)$.*

Proposition 7.2 ([8, Proposition 4.2]). *Let A_1 be the constant in Theorem 7.1. Then we can take $\mathcal{S}^{new}$ so that every prime $\mathfrak{q} \in \mathcal{S}^{new}$ satisfies $\mathrm{N}(\mathfrak{q}) \leq 2d_k^{A_1 h_k}$.*

For a place v of k and an element $\alpha \in k$, define $||\alpha||_v$ as follows.

- If v is finite, let $\mathfrak{q}$ be the prime of k corresponding to v, and let $||\alpha||_v := \mathrm{N}(\mathfrak{q})^{-\mathrm{ord}_{\mathfrak{q}}(\alpha)}$ where $\mathrm{ord}_{\mathfrak{q}}(\alpha)$ is the order of α at $\mathfrak{q}$. Here we put $||\alpha||_v := 0$ if $\alpha = 0$.
- If v is real, let $\tau : k \hookrightarrow \mathbb{R}$ be the embedding corresponding to v, and let $||\alpha||_v := |\tau(\alpha)|$.
- If v is complex, let $\tau : k \hookrightarrow \mathbb{C}$ be one of the embeddings corresponding to v, and let $||\alpha||_v := |\tau(\alpha)|^2$.

For an element $\alpha \in k$, let $\mathrm{H}(\alpha)$ denote the absolute height of α defined by

$$\mathrm{H}(\alpha) := \left(\prod_v \max(1, ||\alpha||_v) \right)^{\frac{1}{n_k}},$$

where v runs through all places of k. We know that there is a positive constant δ_k, depending only on k, such that for every non-zero element $\alpha \in k$ that is not a root of unity we have $\log \mathrm{H}(\alpha) \geq \delta_k / n_k$ (cf. [6, p.70]). Fix such a constant δ_k. Define the constant $C_1(k) := \frac{r_k^{1+r_k} \delta_k^{1-r_k}}{2}$.

Proposition 7.3. *Let $\mathfrak{q}$ be a prime of k. Then there is an element $\alpha'_{\mathfrak{q}} \in \mathcal{O}_k \setminus \{0\}$ which satisfies $\mathfrak{q}^{h_k} = \alpha'_{\mathfrak{q}} \mathcal{O}_k$ and $\mathrm{H}(\alpha'_{\mathfrak{q}}) \leq |\mathrm{Norm}_{k/\mathbb{Q}}(\alpha'_{\mathfrak{q}})|^{\frac{1}{n_k}} \exp(C_1(k) R_k)$.*

Proof. Take an element $\gamma \in \mathcal{O}_k \setminus \{0\}$ which satisfies $\mathfrak{q}^{h_k} = \gamma \mathcal{O}_k$. Then, by [8, Lemme 3], there is an element $u \in \mathcal{O}_k^\times$ satisfying $\mathrm{H}(u\gamma) \leq |\mathrm{Norm}_{k/\mathbb{Q}}(\gamma)|^{\frac{1}{n_k}} \exp(C_1(k) R_k)$. If we put $\alpha'_{\mathfrak{q}} = u\gamma$, then $\mathfrak{q}^{h_k} = \alpha'_{\mathfrak{q}} \mathcal{O}_k$ and $\mathrm{H}(\alpha'_{\mathfrak{q}}) \leq |\mathrm{Norm}_{k/\mathbb{Q}}(u^{-1}\alpha'_{\mathfrak{q}})|^{\frac{1}{n_k}} \exp(C_1(k) R_k) = |\mathrm{Norm}_{k/\mathbb{Q}}(\alpha'_{\mathfrak{q}})|^{\frac{1}{n_k}} \exp(C_1(k) R_k)$. The last equality holds because $\mathrm{Norm}_{k/\mathbb{Q}}(u^{-1}) \in \mathbb{Z}^\times = \{\pm 1\}$.

□

Define the constant $C_2(k) := \exp(24 n_k C_1(k) R_k)$.

Proposition 7.4. *Under the situation in Proposition 7.3, we have* $|(\alpha'_{\mathfrak{q}})^{\varepsilon}| \leq \mathrm{N}(\mathfrak{q})^{24h_k}C_2(k)$ *for any* $\varepsilon \in \mathcal{E}(k)$.

Proof. Let $\varepsilon = \sum_{\sigma\in\mathrm{Gal}(k/\mathbb{Q})} a_\sigma\sigma$. Then

$$|(\alpha'_{\mathfrak{q}})^{\varepsilon}| = \left|\prod_{\sigma\in\mathrm{Gal}(k/\mathbb{Q})}(\alpha'_{\mathfrak{q}})^{a_\sigma\sigma}\right| \leq \left(\prod_{\sigma\in\mathrm{Gal}(k/\mathbb{Q})}\max(1,|(\alpha'_{\mathfrak{q}})^{\sigma}|)\right)^{24} = \prod_{v|\infty}\max(1,||\alpha'_{\mathfrak{q}}||_v)^{24}$$

$$= H(\alpha'_{\mathfrak{q}})^{24n_k} \leq |\mathrm{Norm}_{k/\mathbb{Q}}(\alpha'_{\mathfrak{q}})|^{24}\exp(24n_kC_1(k)R_k) = \mathrm{N}(\mathfrak{q})^{24h_k}C_2(k).$$

Note that the third equality holds because $\alpha'_{\mathfrak{q}} \in \mathcal{O}_k \setminus \{0\}$.

□

For $a > 0$, define the constant $C(k,a) := (a^{24h_k}C_2(k) + a^{12h_k})^{2n_k}$.

Proposition 7.5. *Under the situation in Proposition 7.3, we have* $|\mathrm{Norm}_{k(\beta_{\mathfrak{q}})/\mathbb{Q}}((\alpha'_{\mathfrak{q}})^{\varepsilon} - \beta_{\mathfrak{q}}^{24h_k})| \leq C(k,\mathrm{N}(\mathfrak{q}))$ *for any* $\varepsilon \in \mathcal{E}(k)$ *and any* $\beta_{\mathfrak{q}} \in \mathcal{FR}(\mathrm{N}(\mathfrak{q}))$.

Proof. For any $\tau \in \mathrm{Gal}(k(\beta_{\mathfrak{q}})/\mathbb{Q})$, we have $|((\alpha'_{\mathfrak{q}})^{\varepsilon} - \beta_{\mathfrak{q}}^{24h_k})^{\tau}| \leq |(\alpha'_{\mathfrak{q}})^{\varepsilon\tau}| + |\beta_{\mathfrak{q}}^{24h_k\tau}| \leq \mathrm{N}(\mathfrak{q})^{24h_k}C_2(k) + \mathrm{N}(\mathfrak{q})^{12h_k}$. Then $|\mathrm{Norm}_{k(\beta_{\mathfrak{q}})/\mathbb{Q}}((\alpha'_{\mathfrak{q}})^{\varepsilon} - \beta_{\mathfrak{q}}^{24h_k})| = \prod_{\tau\in\mathrm{Gal}(k(\beta_{\mathfrak{q}})/\mathbb{Q})}|((\alpha'_{\mathfrak{q}})^{\varepsilon} - \beta_{\mathfrak{q}}^{24h_k})^{\tau}| \leq (\mathrm{N}(\mathfrak{q})^{24h_k}C_2(k) + \mathrm{N}(\mathfrak{q})^{12h_k})^{2n_k} = C(k,\mathrm{N}(\mathfrak{q}))$.

□

From now to the end of this section, take $\mathcal{S}^{new}$ as in Proposition 7.2, and take $\alpha_{\mathfrak{q}}$ to be $\alpha'_{\mathfrak{q}}$ in Proposition 7.3 for any $\mathfrak{q} \in \mathcal{S}^{new}$.

Proposition 7.6. *For any* $m \in \mathcal{M}_2^{new}(k)$, *we have* $|m| \leq C(k, 2d_k^{A_1h_k})$.

Proof. We have $m = \mathrm{Norm}_{k(\beta_{\mathfrak{q}})/\mathbb{Q}}(\alpha_{\mathfrak{q}}^{\varepsilon} - \beta_{\mathfrak{q}}^{24h_k})$ for some elements $\mathfrak{q} \in \mathcal{S}^{new}$, $\varepsilon \in \mathcal{E}(k)$ and $\beta_{\mathfrak{q}} \in \mathcal{FR}(\mathrm{N}(\mathfrak{q}))$. Then we obtain $|m| \leq C(k,\mathrm{N}(\mathfrak{q})) \leq C(k, 2d_k^{A_1h_k})$ by Propositions 7.2 and 7.5.

□

Theorem 7.7. *For any* $p \in \mathcal{N}_1^{new}(k)$, *we have* $p \leq C(k, 2d_k^{A_1h_k})$.

Proof. Let $p \in \mathcal{N}_1^{new}(k)$. If $p \in \mathcal{N}_0^{new}(k)$, then $p \leq C(k, 2d_k^{A_1h_k})$. If $p \in \mathcal{T}^{new}(k)$, then $p \leq \max(3, 2d_k^{A_1h_k})$. If $p \in \mathbf{Ram}(k)$, then $p \leq d_k$. Therefore we conclude $p \leq C(k, 2d_k^{A_1h_k})$.

□

References

[1] *K. Arai*, On the Galois images associated to QM-abelian surfaces, Proceedings of the Symposium on Algebraic Number Theory and Related Topics, 165–187, RIMS Kôkyûroku Bessatsu, **B4**, Res. Inst. Math. Sci. (RIMS), Kyoto, 2007.

[2] *K. Arai*, Galois images and modular curves, Proceedings of the Symposium on Algebraic Number Theory and Related Topics, 145–161, RIMS Kôkyûroku Bessatsu, **B32**, Res. Inst. Math. Sci. (RIMS), Kyoto, 2012.

[3] *K. Arai*, Algebraic points on Shimura curves of $\Gamma_0(p)$-type (II), preprint, available at the web page (http://arxiv.org/pdf/1205.3596v2.pdf).

[4] *K. Arai, F. Momose*, Algebraic points on Shimura curves of $\Gamma_0(p)$-type, J. Reine Angew. Math., published online (ahead of print).

[5] *K. Arai, F. Momose*, Errata to Algebraic points on Shimura curves of $\Gamma_0(p)$-type, J. Reine Angew. Math., published online (ahead of print).

[6] *Y. Bugeaud, K. Győry*, Bounds for the solutions of unit equations, Acta Arith. 74 (1996), no. 1, 67–80.

[7] *K. Buzzard*, Integral models of certain Shimura curves, Duke Math. J. **87** (1997), no. 3, 591–612.

[8] *A. David*, Caractère d'isogénie et critères d'irréductibilité, preprint, available at the web page (http://arxiv.org/pdf/1103.3892.pdf).

[9] *B. Jordan*, Points on Shimura curves rational over number fields, J. Reine Angew. Math. **371** (1986), 92–114.

[10] *A. Kurihara*, On some examples of equations defining Shimura curves and the Mumford uniformization, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **25** (1979), no. 3, 277–300.

[11] *J. C. Lagarias, H. L. Montgomery, A. M. Odlyzko*, A bound for the least prime ideal in the Chebotarev density theorem, Invent. Math. 54 (1979), no. 3, 271–296.

[12] *B. Mazur*, Rational isogenies of prime degree (with an appendix by D. Goldfeld), Invent. Math. **44** (1978), no. 2, 129–162.

[13] *F. Momose*, Isogenies of prime degree over number fields, Compositio Math. **97** (1995), no. 3, 329–348.

[14] *G. Shimura*, On the real points of an arithmetic quotient of a bounded symmetric domain, Math. Ann. **215** (1975), 135–164.

[15] *A. Weil*, Basic number theory, Reprint of the second (1973) edition. Classics in Mathematics. Springer-Verlag, Berlin, 1995.

(Keisuke Arai) Department of Mathematics, School of Engineering, Tokyo Denki University, 5 Senju Asahi-cho, Adachi-ku, Tokyo 120-8551 Japan

E-mail address: `araik@mail.dendai.ac.jp`